REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-xx-2011	Master of Military Studies Research Paper	September 2010 - May 2011

4. TITLE AND SUBTITLE
Leveraging to Win:
The Marine Corps Confronts the "Intelligence Challenges" of Social Media versus Operations Security

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Kozacek, Kevin T.

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
Social media provides opportunities for training, recruiting and information sharing while at the same time heightening the risk of sensitive information release. This paper argues that in order for the Marine Corps to balance social media capabilities it must also limit the risk to operations security, and that to do so it must establish a training program using a developed "tier system" to assist in mitigating the risk while providing additional information resources to the end user.

15. SUBJECT TERMS
Social media, operations security, OPSEC

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass	UU	44	19b. TELEPONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

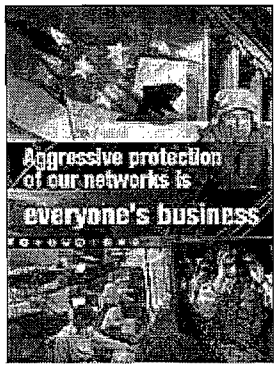
MASTER OF MILITARY STUDIES

Leveraging to Win:
The Marine Corps Confronts the "Intelligence Challenges" of Social Media versus Operations Security

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

KEVIN T. KOZACEK

AY 10-11



Mentor and Oral Defense Committee Member: J. W. Sarden
Approved:
Date: June 2011

Oral Defense Committee Member: D. F. GITNER
Approved:
Date: 3 June 2011

Executive Summary

Title: Leveraging to Win: The Marine Corps Confronts the "Intelligence Challenges" of Social Media versus Operations Security.

Author: Kevin T. Kozacek, Federal Bureau of Investigation

Thesis: Social media provides opportunities for training, recruiting and information sharing while at the same time heightening the risk of sensitive information release. This paper argues that in order for the Marine Corps to balance social media capabilities it must also limit the risk to operations security, and that to do so it must establish a training program using a developed "tier system" to assist in mitigating the risk while providing additional information resources to the end user.

Discussion: Social media, or the ability to share data with communities of people electronically, is linked to networking powerhouses such as Facebook, with an estimated 517 million users [1]. Facebook has been tied directly to assisting the governmental change in Egypt of 2011. The United States has established itself as the leader in social media use based on the survey conducted by Alexa web information company[2]. A review of recent statistics shows that of the top 10 websites visited in the United States, a social media site was visited 40% more frequently than other sites (Quantcast 2010). The United States military was slow to grasp the power of social media but has recently begun to respect this technology, thus exposing itself to the risks as well as the rewards provided. The military has to deal with many issues concerning the use of social media, not least of which is operations security. Operations security is defined as the security of the military forces and is of foremost concern to the military. The popularity of social media during this time of war has been increasing and everything related to mass information sharing requires scrutiny.

Conclusion: The Department of Defense was arguably late in accepting social media as a legitimate warfare tool. Since 2006 it has made great strides to not only recognize this technology as a tool but respect it enough to actively utilize its capabilities. In particular the Marine Corps, probably the most scrutinized service in the media for its strict handling of social media because of their 2009 notification[3], has responded the quickest by both eliminating social media on government computers then allowing it with restrictions. Research in developing this paper was able to provide evidence that the handling was appropriate for what the Marine Corps was attempting to do at that time and shows promise for the future. The same research identified new options for military members once they return from assignments. One benefit identified has been the Veterans' Administration (VA), which has taken strides to ensure that the administration is aware of the social media products available to the veterans[4]. The VA's use of social media aids in providing information, conducting training and consulting. This style of progression is heralding in the next chapter in the war fighter's life. The Marine Corps has taken the steps to integrate social media into its environment by establishing official Facebook and Twitter accounts to keep interested personnel updated. However, the Marine Corps has yet to identify a mitigator to the risk social media provides to operations security. The current operating procedure for the Marines is to complete an online course that teaches them the security risks associated with divulging too much personal information. This requirement is a

step in the right direction for the Marine Corps, but its presentation via computer training evolution and a quiz is easily bypassed without retention of information.

The information gathered on social media's effects on operation security was used to determine each Marine's comprehension. Social media can provide unique capabilities to the Marine Corps and it is now a mission objective to recognize the benefits social media provides and mitigate out the risks to operations security the media presents. The use of social media as an intelligence gathering system can be exploited by those wanting to do harm to the Marine Corps or with appropriate training, social media can be used to disseminate large amounts of information to identified groups quickly. Adequate training in operations security with emphasis placed on social media will prepare the Marine Corps for operations in a cyber environment.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENT AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATIONS FROM, ABSTRACTIONS FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

Page

Table of Contents

Page

Preface

This study was inspired out of concern that the Marine Corps needed to do a better job of dealing with social media. Guiding this approach was the assessment that the Marine Corps' initial reaction of eliminating social media from its computers all together was an overreaction to a source that had not been completely discovered yet. This would be similar to an individual shutting down his or her internet access because of reading that hackers are attempting to gather personal information via the internet. Social media provides its users with a unique opportunity to communicate and share data in real time while never needing too actually see the person. As I read up on the Marine Corps reaction to social media, I was shocked that it would eliminate its own Marines' abilities to communicate with friends and family. A first step was to look at how the Marine Corps sees operations security and its relationship to the release of personal identifiable information. What kind of training was provided? Indeed, one of the first items I noticed was the lack of adequate training for the level of knowledge that the newer generation of Marines is bringing. In order to gather data for my hypothesis I sent out a survey to a group of Marines with questions on their use and understanding of social media. The data provided suggested that a large number of the Marines surveyed had access to and used social media at least on a weekly basis. Those that used social media in a combat environment had used it from government computers and mostly as the sole form of communication to friends and family stateside. This group is a direct demographic of the type of Marine using social media. The group has an understanding at a high level of operations security and an above average use of social media yet the Marine Corps provides training not to build on their level of understanding but at a minimum level. In order to address this issue I recommend a tier level of training with each tier providing more access, via government computers, to social media and other internet sites. Those Marines that require access to these sites as a part of their daily duties will need to complete the tiers as required.

"As recent protests swept across the Middle East and North Africa — from Tunisia and Egypt to Libya and Yemen — dissidents used social media sites such as Facebook, Twitter and YouTube to organize anti-government demonstrations."

Lolita C. Baldor and Darlene Superville (AP)
May 16, 2011

"Helicopter hovering above Abbottabad at 1AM (is a rare event).... The few people online at this time of the night are saying one of the copters was not Pakistani...."

Sohaib Athar (via Twitter)
May 1, 2011

"People are getting Article 15s for what happens on Facebook, MySpace and YouTube."

Selena Coppa (Military Blogger)
July 18, 2009

Hardly a day goes by without some mention of what "social media" – Facebook, Flickr, Twitter – can do. The above quotes are recent examples at the power of social media and its use. But how should the Marine Corps, an institution that must maintain a commitment to operations security, deal with this new capability? "Social media" is defined as *forms of electronic communication (as Web sites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (as video)* [5]. The word "media" is the plural of medium, which is the venue used in order to communicate with the objective of influencing people. The media most popular today vary from web-based activities (requiring a browser) to mobile technologies. Social media provides opportunities for training, recruiting and information sharing while at the same time heightening the risk of sensitive information release. This paper argues that in order for the Marine Corps to balance social media capabilities it must also limit the risk to operations security (or OPSEC),

and that to do that it must establish a training program using a developed "tier system" to assist in mitigating the risk while providing additional information resources to the end user. These tier systems will help eliminate the "grey area" between the Marine Corps protecting its brand in the cyber world and leaving that responsibility elsewhere.

This MMS paper advances the Marine Corps' view on future warfare, and how the use of social media can both assist and hurt the Marine Corps. This examination will evaluate the individual Marine's assessment of the Marine Corps operation security plan for social media and the Marine's use of social media. Guiding this approach is the concern that the Marine Corps' initial reaction, that of eliminating social media from its computers all together, was an overreaction to a source that had not been completely discovered yet.

The foundation of social media is based in a "cyber world" (an online world where users have the mechanisms in place to transact any business or personal activity as easily and freely as they can transact them in the physical world[6]) of virtual environments consisting of everything from online education institutions to millions of "hackers" (a person who illegally gains access to information on a computer[7]). The Secretary of Defense has vested control of this area of operation in USCYBERCOM (United States Cyber Command), which is a joint service, sub unified command headed by the Army's General Keith Alexander. General Alexander's belief in "cyber" as a war-fighting tool was made clear when he stated, "Cyberspace has become a critical enabler for all elements of national and military power," in remarks delivered on June 3, 2010, at the Center for Strategic and International Studies. USCYBERCOM's mission is directly associated with the opportunities that social media presents in the way of network

vulnerabilities like viruses, hacking and sniffers. Turning some Marines into "Cyber Marines"[8] (Marines that are trained in the defense principles of virtual battlefield) is what the leadership of the Marine Corps has reported to Congress it intends to do, but the responsibility for network security should fall on all Marines and not just the few selected to work within USCYBERCOM.

In order to access any web-based activities the user needs internet access, which has been a concern of the current Administration. During the January 25, 2011, State of the Union address, President Barrack Obama solidified a five-year path that intends for 98% of US citizens to have access to wireless high-speed internet by the end of 2016.[9] But how to achieve this goal and how can the Marine Corps leverage this capability?

The body of this paper will discuss the process of selecting a group of individual Marines that will represent the Marine Corps and gathering information from these Marines on their use of social media and understanding of operations security. Following the breakdown will be a review on the history of social media with emphasis on the Marine Corps and Department of Defense. The final portion of the paper is tying together how social media is affecting the Marine Corps and what the Marine Corps could do in order to limit the risk to operations security.

METHODOLOGY

One of the key areas of a commander's focus must be the threat that social media presents to the OPSEC of the forces. To help evaluate this threat from the Marine's prospective, a qualitative method[i] approach was used. In order to get an understanding of this fundamental need, in-person interviews and social media have been used as the sources for obtaining responses from the individual Marines in the target audience. The use of social media forms like Facebook and media blogs were used in place of a personal interview to reach troops in various areas of the world including those deployed to war zones.

Targeting Group

Utilizing social media as primary method for gathering data allowed the author to talk directly to those troops that actively use social media. This direct connectivity benefited the research in two ways. The first was to be able to reach a large population of military members with a single, standard evaluation. The second allowed for the member to reflect on the questions and answer them on their own time and without disruption to their everyday duties. The target group selected ranged in location, age, military experience, pay grade and levels of understanding of OPSEC and social media. The responses from those interviewed and those that responded via a social media forum are held in confidence to ensure honest responses to questions. In order to gather more data, interviews were conducted in person and on the phone; responses were dictated via handwritten format.

Collection Techniques

[i] Kvale, Steinar. Interviews An Introduction to Qualitative Research Interviewing, Sage Publications, 1996

The interviews conducted in-person and via the telephone consisted of a series of questions related to both the group's use of social media and their understanding of operations security. Eleven questions had been asked and a copy of the standard questionnaire is attached as Appendix A. In order to receive honest responses, anonymity has been provided to each of the target members and they were informed that the interview was strictly for educational purposes[ii]. As an additional resource for gathering more information on the use of social media, social networking sites were searched to review online forums. These forums assisted in identifying some of the social media resources used and the user's responses to removing or limiting the military members' access to these sites.

Data Review

Upon completion of the collection stage, the review process began to place data into usable fields. The usable fields in this study consisted of those interviewed that used social media weekly, those that used social media while forward deployed and the level of military experience each interviewee possessed. The focus of the data review was to identify members that use or are familiar with social media, and of those users which of them consider OPSEC while they exchange information.

Limitations of Study

The limitations of the study resulted from any number of coordinating issues that resulted in people not able to complete the survey due to military operations or simply shifting of schedules due to everyday issues. The study had originally suggested comments from one hundred Marines of various backgrounds and experiences. It was realized that with the amount

[ii] The data collected has been retained without any identification of the target member

of time required to gather and review data, conform questions, and schedule interviews for one hundred people it would take longer than allotted for the research. Recommendations for future studies on this topic suggest a longer evaluation period and utilize the benefits of social media and social networking in order to gather or deliberate data.

In order to counter this limitation, research was viewed from previously conducted studies to compare results. Informal web polls were also reviewed to gather data and compare results, as were various news articles and reports.

LITERATURE REVIEW

The History of Social Media

The information-sharing explosion labeled social media provides users a route to express themselves and provide information to a wide range of audiences. For the extent of this research, social media began from the Web 2.0[10], which defined the interactive facet of websites. In Web 2.0, a format called Really Simple Syndication (RSS) can allow website users to be notified anytime an update has been added to that headline. This format had an immediate impact because interested users are able to keep abreast on ever-changing topics from blogging updates of an individual to topics from a larger news source. Internet marketers are able to track any number of user's information from websites a user frequents, such as online news articles, to the time a user spends reading them. The better understanding of the consumer has assisted marketing analysts in moving toward more direct advertisements and search targets but this acquired data also encroaches upon a user's personal and identifiable information. The Marine Corps could benefit from this business approach to social media by gathering data (via site

surveys) from users of their media. Understanding who the Marine Corps target audience is for a given media will allow better-targeted information directed at that group.

Social media has quickly branched out to users' ability to network with other people using social networking sites (SNS). Understanding the foundation of social media will assist in knowing where this technology will lead. Being able to have an understanding of where this media can lead will help the Marine Corps to establish both security measures and technical advances. One inescapable factor that the Marine Corps must work with will be continuous advancements in media technology. The pathway for social media, as these advancements progress, will continue to adjust and users will redefine the abilities of social media. To solidify this point, the paper will offer examples of the risk and reward factors of this technology.

Social media as a powerful tool for exchanging information will likely impact future military operations by providing the military a more transparent online appearance. Military personnel posting updates to Facebook accounts or posting information to blogs is the most likely way that this information gets out. Social media has provided users with simple and immediate updates of personal reviews of world issues and used to organize high profile events such as impromptu political speeches and gatherings. For instance, the citizens in Egypt have voiced their opinions about their government and the rest of the world received these first person accounts via social media[11]. The Egyptians were able to find like-minded pockets of people via these networks and organize an impromptu gathering to voice their opinion against the government. As stated by Andrew Sullivan on June 13, 2009, "The revolution will be Twittered." As never before, the world was able to see firsthand accounts of the revolution and

major news sources used individual online reports to spread the news. The military must understand that social media as an intelligence gathering system, has the capabilities to topple long-standing governments. This is the immediate threat to the Marine Corps.

The Marine Corps and Social Media

The military first experienced the social media trend in 1997[12] when a large percentage of military members received access to the Internet from government computers. More recently the Marine Corps has recently shown concern with SNS defined as "web-based services that allow communities of people to share common interests and/or experiences (existing outside of DoD networks) or for those who want to explore interests and background different from their own...."[13] Tied into the SNS concern is its Internet Based Capabilities, which the Marine Corps defines as:

> "all publicly accessible information capabilities and applications available across the internet in locations not owed, operated, or controlled by the Marine Corps, Department of the Navy (DON), Department of Defense (D[o]D), or the Federal Government. Internet-based capabilities include collaborative tools such as social networking sites, social media, user-generated content, social software, email, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps). (para. 6)"[14]

Younger generations are the major consumers of technology and also the target groups that the military is recruiting to fill the ranks of tomorrow's military. In order for the military to communicate with these groups, it needs to exchange information through all forms of media. An article published online at www.suite101.com by Kelly Sharp stated:

> "The biggest challenge for some managers may be the insistence that Gen Y [generation Y – born after 1982] has for electronic communication. Text messaging is a normal form of communication for this group, as is the social networking found on the Internet. Telling a Gen Y employee she cannot search the net or talk to her friends on Facebook at work may result in a stunned

> expression. For this generation, the Internet and texting are the phone conversations of yesteryear (Sharp 2009)."[15]

It was the generation born in and after 1982 that incorporated the social media scene into everyday life. "Millennials,"[16] as they are referred to, joined the Marine Corps and quickly incorporated the social media scene into the service life. The new generation of social media users already has expectations of their work environments. One is to send and receive information quickly and freely within the realms of their everyday duties. This could be as simple as updating their Facebook or Twitter accounts or expressing beliefs about current affairs. The Marine Corps must actively utilize these forms of media to ensure that their "brand" is being projected to these technology-guided people.

The Marine Corps has examples of operational information shared openly, as seen through the numerous You Tube video uploads from troops on the frontline of the Global War on Terrorism (GWOT). A recent view of some uploaded footage[17] identifies the unit, in this case 1st Battalion, 6th Marines, which shows the Marines in a firefight as well as patrolling a local village. The Marines are seen exchanging gunfire in one scene and giving candy to local children in the next. The operations security (OPSEC) issue here is the scene in which the patch on the center of the flak jacket identifies the individual as a military member with rank and service affiliation. Identifying military members is cause for concern but the video briefly shows the interpreter who could be subject to retaliation[18]. This instant freelance type of reporting can come with costs to those depicted in the videos and pictures. Names of Marines and units will be identified as well as equipment being used, locations in which the service members are operating and local nationals who appear to be assisting the United States (US) Military.

Social media is an extraordinary way to gather information, pass related news and recruit new members to its ranks. A recent poll [see Appendix B] shows that 77% of North America has access to the Internet, which equates to around 266 million people[19]. A continuation of a similar poll [see Appendix C] goes on to state that 149 million users in the United States have a Facebook account[20]. These stats provide dramatic accounts of the sheer numbers that the Marine Corps could be communicating with via the use of social media.

The military makes available to its service members the equipment, training and tools that provide support to assist in reaching the military's final operational endstate. Social media's use as a cost effective way to distribute needed information through the 77% of North Americans with access to the internet could prove useful in the ever-changing environment of pre-deployment build-ups. This would allow the ability to provide training like language instruction, to the service members before they deploy to a combat zone. An example of the kind of information exchanged via social media would be which items beyond military issued equipment current troops in zone would recommend to replacement troops[21].

Bringing a personal laptop with an Internet connection to a combat environment (with units' authorization) could assist the member in continual communication with friends and family. This raises concern in relation to OPSEC, because this communication could relay identification of inbound and exiting troops. Other information that could be shared are articles that could be used as trading items. Deployed troops often encounter the local nationals and articles of US service member are highly sought after and could be used as bargaining tools.

Using online applications for smart phones, users are able to sharpen their brainpower with language processing and decision making fitness programs[22]. A new application allows service members the ability to update and track their mental health evaluations. There are common sets of factors that can affect the service member and the application asks ten anchor questions about each issue to allow the user to express how that issue makes them feel[23]. The ability to track this information for the user eliminates the risk of losing paper-based products or relying on the member to recall each scenario. While these programs are beneficial to the service and service members, given the opportunity to hack personal medical information would be an ideal goal for a trained hacker. In order to defend this service member must know to what extent of unit and personal information they can safely divulge and this is accomplished through training.

Social media has been a player in the current battlefield and will continue to play a factor as new missions and applications present themselves. The best way for the military to evolve with the use of social media is to accept the risks with mitigation and adapt new technologies like Smart Phone applications to battlefield troops[iii]. Operations security has been compromised in the past and the military must expect it will be compromised in the future. The best option in order to continue to communicate[24] with the next generation of war fighters is to provide better training to the troops and plan for future releases of sensitive information via social media. One way to ensure this scenario will be taken seriously will be to apply strict punishments to those who violate rules. Make every Marine a reporter of violations (including those of troops and family members) and the masses will police themselves. In the event that accounts are hacked or

[iii] The US Army has conducted many studies as to the prospects of Smartphone applications and their benefits to today's war fighter. In order to stay in the realm of the Marine Corps, however, this study focused more narrowly on the Naval Services of the Navy and the Marine Corps.

an identity stolen, then the military member and military representative work to assist the individual with both the civilian and military process while identifying any training shortfalls.

The Marine Corps needs to utilize social media as a main effort to keep interested parties up to date about the current and identified needs. The Marine Corps must take immediate action on whatever false information (misinformation) is reported via online sites. Catching all misinformation is next to impossible but with particular concentration directed to sites that received a high number of internet traffic. When dealing with misinformation the Marine Corps must be swift and accurate with their response. Not responding to misinformation could give the appearance that the information in question is true. The use of social media can assist the Marine Corps by instantly providing information authorized for public release. The interested parties on the official Marine Corps social media sites will be easy to provide with information. The unofficial sites should pose great concern of misinformation. If the Marine Corps could actively search the popular unofficial sites for misleading information and redirect the readers to the official site it will help the information sharing battle in the cyber world.

The Marine Corps was not ready for the risks social media provided like the anonymity of the writers and a sense of comfort because of the lack of physical interaction. As a result, in August of 2009[25], the Marine Corps issued an order (MARADMIN 0458/09) banning the use of social media on official computers. The ban was put into effect because, as was stated, "[social media and social networking sites] in general are a proven haven for malicious actors and content and are particularly high risk due to information exposure, user generated content and targeting by adversaries[26]". The MARADMIN stated that Marines could not use social media from computers on the Marine Corps unclassified system. This was a great opportunity missed

to leverage social media and embrace the technology because the Marines made utilizing this media against regulations, thus shutting down further interest from Marines. Instead, the order eliminated Marines' access to social media via official computers. The order was necessary because of the risk to OPSEC, but the Marine Corps could have saved some harsh critics had it highlighted that access via non-official computers was unimpeded.

The effect of this was the Marine Corps quickly received scrutiny for not realizing that eliminating social networking sites via official computers was eliminating a major source of communication between Marines on the frontline and their friends and family in the US. While the Marines had been willing to make sacrifices for operational security, the capabilities of social media as a morale factor provided reasons to continue the freedom of use. The Marine Corps realized that its order was only effective to those individuals that used forms of social media at work and on official computers. Research proves this to be a relatively a small portion of the Marine Corps. There was a population of Marines with access to non-official computers and the information they had been exchanging was virtually unfiltered. The unmentioned part of the order that left a large hole to be filled was the posting of Personally Identifiable Information (PII) via any computers. It is the belief of this author that the Marine Corps did this because the avenues one would have to go through in order to gain access to the various sites was time consuming and impossible unless the intruder already had access. The Marines who used social media had multiple ways to access sites whether on (smart) telephones, personal computers or Internet cafes provided in some frontline bases. The Marine Corps concern was of course that OPSEC. The concern with OPSEC is present with or without social media's ability to transmit data. Anyone with access to critical information has multiple ways of getting that information to

others with both need to know and those without. Making copies and handing the copies out is one way that has worked for many espionage cases; social media though, provides a unique ability to transfer data quickly and to numerous people at a single time. Social media has been the prime area of attention in the past because it is popular and easy to use[27]. The popularity of social media also makes it a target for the criminal mind that wishes harm against the US Government.

The Marine Corps has always been concerned with OPSEC and, through education and training, has greatly mitigated this concern. The unique problems that social media presents are as described before: anonymity of information release and a false sense of security because of the lack of physical interaction. The leadership's focus of concern should not be about Marines letting classified information slip, since Marines are regarded as well informed about what information should and should not be released outside the military. Instead, an adversary will attempt to gather small pieces of information from a variety of sources and then begin to piece together troop association and movement activities or information that is more vital. This is why the training needs to be focused on a larger lens which will allow the Marines to see probes in a bigger picture.

While there are threats present with the use of such media, training users in the correct security measures appears to be a satisfactory answer for the military. The major training issue is that Marines are required to complete a once a year Personal Identifiable Information (PII) course via an online training source (DISA 2010) that can be taken and passed without testing for information retention. There is testing throughout the course, but if the participant answers the

question wrong the computer tells the user he or she is wrong, provides them with the correct response, and finally re-asks the question. A more proficient way of testing would be to ask questions directly after major talking points[iv]. If the user gets the question wrong, he/she is sent back to the beginning of the section to review the material again. A similar question can be posed to the user on a second review. In the event the user fails the question, they move on with the failure annotated in their final report. Too many failures on any training section would cause the user to fail to get credit for the course with remedial training scheduled. The remedial training can still be CPU based but will ask more questions and direct the user's attention to the lesson materials. In the event that the user fails, then their CPU access is limited and any work related effects will be noted in a performance evaluation. The idea of the training will not be to allow everyone the ability to pass the course; instead, focus is directed to identify areas of concern with PII. Information will be captured to gather common areas of concern and modifications made to future training material.

After a short review process, the Marine Corps leadership within the information technology arena determined that risks associated with social media could be mitigated. In the original Marine Administration Message (MARADMIN 0458/09), the Marine Corps only disapproved access to social media sites on unclassified government computers. Information, much of which was powered by social networking, made the American people believe that Marines could not access social media sites. This was far from true as proven by the Marines in Afghanistan because the military established a separate network for the Marines personal use (Graham, 2009)[28] to include computers at certain locations. By not clearly identifying and

[iv] The idea of this type of distant learning is nothing new: the basic outline of this testing is currently being utilized in the State of Pennsylvania's K-12 grade. http://www.padistance.org/index.html

rectifying the social media "buzz" on this order, the Marine Corps was forced to conduct some public relations activities.

The Marine Corps had to defend its policy publicly for the handling of the social media situation when in reality; it handled the issue of restricting access on official computers the same way most employers did in America. It was instead a simple misunderstanding of the order. American's belief was that the Marines stated that they could no longer have access to SNS and social media leaving many families of deployed Marines in fear that they would have to resort back to "snail mail." This should have been a lesson for the Marine Corps about the power of social media as the Marine Corps ended up defending a MARADMIN to the public. Numerous media outlets with concern on the order interviewed the office of public affairs in the Marine Corps. While the Marines stood by their order, it was in the process of re-evaluating the order with other entities of DoD.

In February, the Department of Defense put out a formal policy labeled "Responsible and Effective Use of Internet-Based Capabilities" (Lynn 2010) that replaced the MARADMIN of 2009. In reality, the American Public took out of context the initial impression[29] that the Marine Corps eliminated the Marines access to social media. There was one stipulation in the 0458/09 policy that allowed for use of social media on government computers and it was via the digital waiver[30]. Sergeant Major Carlton W. Kent made the following statement, "Social media is clearly becoming a way of life for today's younger Marines". Kent further stated "So many Marines are utilizing these sites, and this is just another tool to help spread the word and inform Marines on important topics"[31], further bolstering the Marine Corps backing of social media.

In March of 2010, MARADMIN 181/10 removed the ban on social media. The new order defined that Marines who access the sites must only use it for "reasonable durations and frequency" and under the authorization of a superior[32]. The PII was still a standard for training but it left a void in tying together social media's use and the possible negative outcomes. Above all this order left the responsibility of authorization to a superior who depending on their access to social media have no more knowledge on its risks. While the new order is a step in the right direct there is still more training that could be provided in order to ensure the Marines are appropriately adapting to the order.

Department of Defense's "Official Sites"

The military has taken a long look at successful corporations and evaluated their success in using various social media markets. In a study conducted by the public relations firm Burson-Marsteller, it was found that 79 percent of the largest 100 (of the Fortune 500) companies use Facebook, Twitter or YouTube; and many have more than four Twitter accounts[33]. The results provide statistical data linking the use of social networking and success in the business world. The military should learn from corporations that social media markets are important because they are providing an unfiltered source of information to interested parties. Protecting the brand of the military on social media sites should be a goal that the military is striving for in the social media environment. .

The Department of Defense (DoD) established a Directive Type Memorandum 09-026 concerning its use of social media and has endorsed the abilities this technology provides to the

21st century fighting force. In the past three years, military commands are now operating Facebook sites and updating operating procedures via Twitter accounts. One operating procedure the DoD has placed on its military sites is that they must register[34] with the Assistant Secretary of Defense for public affairs. The DoD even went so far as to label such sites as 'official external presence.' (Department of Defense 2011) This new procedure for identifing official sites has assisted the general public in getting correct and accurate information about Defense related subjects.

The DoD has begun its approach in using social media as a tool that could benefit the services. The next step is determining how the DoD will evolve with social media. This evolution has begun happening in the services as they all have officially approved and monitored social media sites. An example of how this works in the Marine Corps is assigning Marines and their families to new duty stations in another state. In a social media driven environment, provided to the Marine is a list of sites that provide information on the new location. These sites can vary from housing locations to schools. The sites have other people's comments that have been in the scenario that the Marine and family will be going through. With a simple register of the site notification, the new family can get updates from the site.

One of the foundations of the DoD is that leadership makes decisions and the subordinates put these decisions into action. Senior leadership has granted the use of social media and networking and with that, we have seen numerous commands following suit. In the Marine Corps alone, one will note there is one official Facebook page dedicated to the Marine Corps. Looking deeper on January 21, 2011, it was noted that Facebook had over 188 sites

dedicated to various units, Twitter had another 33, Flickr had 20 and YouTube had another 17 (Marines.mil 2011). To further bolster this point, in a little over two months (May and June of 2009) the Facebook page for US members in Afghanistan received over 20,000 new members[35]. This means that military members, their friends, families, and any other interested party, will closely follow the overseas operations of Marines

One of the better uses of social media by the forces is countering any kind of disinformation reported by unofficial sources. An example of this type of countering was in June of 2009, when an improvised explosive device (IED) attacked Combined Joint Task Force 82. As local civilians gathered to view the damage from the IED, insurgents tossed grenades into the crowd. Before the troops could return to base, one of the insurgents uploaded pictures to make it look like the US Military killed civilians with the grenades. The military was able to gather video that showed the insurgent tossing those grenades into the crowd of civilians[36]. The military has also recently used social media sites to pass information about troop rotations to assist in keeping members informed[37].

Expectations are low that the military could thwart every attempt to tarnish the image of the forces via social media but by using official sites, they can keep accurate information flowing from accredited sources. The forces in the battle space are expected to update their sites so those concerned can have the most truthful source for information. The more information provided, the less chance there would be for people to gather news and information from other media sources whose agenda is to get and increase ratings. While not all information is appropriate for public release due to the security and safety of our forces, the Marine Corps must continue to

maintain awareness of information reported in the media. Reviewing the information will assist in identifying information leaks and will assist the Marine Corps in becoming more transparent.

RESULTS

Qualitative Research

When dealing with deploying Marines in an oversea cycle like the Marine Corps' current environment, an information gatherer must be prepared to deal with competing interests. The interview process coupled with the questionnaire allowed a broad range of subjects to provide input into this research as well as gathering data from subjects otherwise unreachable due to deployments. The results provided a number of expected responses as well as a clear understanding that the Marines have engaged a strong operations security plan otherwise in question at the beginning of this research.

All participants interviewed in this case study stated that they understood OPSEC and the risks it provides to the Marine Corps as well as other Operating Forces. The Marines in the target group answered the questions about their training in OPSEC as having had training but also agreed that more training was necessary. Interviews identified the need for actual case studies in which OPSEC, what the violations were and how that information was used against the forces. Newer case studies can be implemented into annual required courses to assist in reducing or eliminating the risk social media provides to OPSEC.

Breakdown:

In today's environment with the current operations in Afghanistan and the experience in Iraq, locating Marines that could speak of their social media use while deployed was not difficult, as each possessed deployed experience. The interviewee talked about his/her experiences while both deployed and in garrison (not deployed). All subjects interviewed possessed at minimum a Facebook page and provided updates to that account at least weekly and in most cases daily. Updating even continued while Marines were in the field and during these times, communication via social media was the preferred and most expedient method. These Marines used social networking to keep a large amount of interested friends, colleagues and family members (annotated as Friends in Facebook) up to date on day-to-day activities while deployed. Facebook provided an all-in-one notification tool because subjects could send a message to all friends or a quick note to only those the user selects. The Marines routinely provided bits of PII but never to the extent had they believed enemies could utilize this information against them. On occasion, during the interview process the subject would attest that they never provided PII on a social media platform but through further discussions would admit to providing locations of their force as well as others.

The fact that the Marines answered in the affirmative in understanding OPSEC and PII but during the same meeting discussed their own potential violations of each draws a conclusion that the training provided to the forces requires modification. The Marines answered that they understand OPSEC and PII because they have passed the online quizzes (PII training required annually by DoD) and attended verbal briefings (not required but various units held this training). This gives the Marines a false sense of security. Every one of the Marines interviewed had a strong affiliation to their sense of security awareness and the associations they kept online.

The conclusion drawn is that the Marines need real life examples of how PII, found online, can be used against the forces. The target group Marines have been using social media for so long that they have developed a barrier of online trust. This trust has been established from what is believed to be a long experience without seeing any effects. Some real time examples of PII used criminally would allow Marines the opportunity to see how a criminal minded individual utilizes simple PII. The target group is well informed to the level of training they are given but desire more direct training. The current OPSEC training will keep good people from making simple mistakes but the world of social media is getting technically more difficult. The next level of training needs to extend into the users online profiles displaying how different pieces of information can be compiled to draw out incredible amounts of data. In a "Red Team" example, a terrorist operative "1" finds a YouTube video of a unit deployed in Iraq. The video shows members of the unit with nametags on the uniforms. From the names, Operative "1" searches Twitter and finds an account for one of the members. Operative "1" joins the member's tweets and follows the member's movements. Operative "1" holds a Twitter account with a non-identifying name and starts to solicit information like pictures and links that can have GPS coordinates attached giving the location certain pictures. Names of other members provide a link to additional information sources. The more sources the better chances operative "1" will gather information pertaining to unit rotation, capabilities, and personnel.

DISCUSSIONS

Social media provides opportunities for training, recruiting and information sharing while at the same time heightening the risk of sensitive information release. This paper argues that an OPSEC "tier" training program could assist the Marine Corps in balancing social media capabilities with its risks. The interviews with the target group provided guidance that suggests that the Marine Corps has adopted a level of training that does not meet the degree of knowledge possessed by the staff. This creates a "grey area" between where the Marines are, where the Marine Corps wants them to be and where the training teaches them too. This gap is filled by building on the foundation of the current training with a more detailed course targeted at the next level of use with social media.

The threats that social media presents are numerous but with appropriate levels of training, they can be mitigated. The more training provided the more individual Marines would start to identify issues and address the issues before any loss of sensitive information. Training is the best way to ensure that the Marines are safely and smartly using social media.

Differences from breakdown elements

Throughout the research the main topic of concern from the individual Marine's perspective seemed to center around the Marine Corps initial response to (2009) the SNS. This appeared to divide the research group between those deployed during that period and those back in garrison. The Marines' deployed viewed the SNS response as the Marine Corps eliminating the Marines main form of communication and in most cases the only form of communication they used. The Marines' in garrison did not feel the same amount of hate because in garrison they had other means of communication via personal cell phones, laptops and internet cafes. The

research identified that the 2009 SNS decision caused serious morale issues to those deployed compared to those that were not. SNS provided some Marines the instant form of mail from friends and family that assisted the Marines in getting through various deployed issues. While the 2009 order was in effect, the Marines resorted back to expensive phone calls and stamped mail. Each Marine interviewed adapted to the requirements of the order but had serious concerns on explaining to loved ones that the everyday updates via VOIP was no longer available.

Similarities from breakdown elements

One of the most consistent questions that the Marines all responded similarly to was the question regarding further training on PII and OPSEC. They even recommended OPSEC and PII training for family members. The fact that these Marines have identified further security issues provides proof that they are currently above the level of training PII provides them. The average Marine has at least a basic understanding of social media and an above average understanding of OPSEC it is now time to provide training that expands on their knowledge.

Final Thoughts

This research project has shown that many functions of the Marine Corps' day-to-day activities provide front-page news. The interested parties vary from citizens within the United States to those groups that look to hurt and exploit the military from any location in the world. Each Marine is a public figure whose comments will reflect directly to the Marine Corps. The Marine Corps should put forth more training to allow the Marines to know the bounders of their comments and PII training will be a step in the right direction.

The original understanding of the Marine Corps PII training was that it was far outdated for the activities Marines are currently pursuing. Through the research process, it was discovered that while more has been requested of the training it indeed does fulfill the minimum requirements of the Marine Corps. Each newer generation will come equipped with updated knowledge of such technology; in order to ensure training is equivalent the Marine Corps should cater to the "social media evolution." This could be completed by designing tiers of PII training designated for those with basic knowledge and a separate course for advanced understanding. Passing each of these tiers will allow the individual the opportunity to access more websites via government computers and with the use of their CAC (Common Access Card). The Marine Corps needs to adapt the testing method for course comprehension, design a test with at least thirty questions to be cycled through each time the test is taken. As it stands now the Marines are tested and retested with the same questions, leaving them the ability to eliminate their previous response.

Recommendations for further studies

Future research projects should focus on particular groups of military members with specifics in deployed versus non-deployed. This project provided a very high-level review of OPSEC understanding of a small number of active duty Marines with deployed status. As this project concluded, it was clear there is a very different understanding of deployed activities, some Marines deployed to established bases and others deployed to the front lines. Establish a questionnaire and provide that to a deployed unit as a whole. This will allow the data gather to establish a standard set of responses for those in the target group. Then the questionnaire should be sent to a similar unit that is not deployed and compare the responses. It would be the author's

assumption that deployed Marines are more dependent on SNS and in turn are more likely to violate OPSEC or release PII in their conversations.

One final recommendation would be to breakdown the research group into different categories like age, technology experience, grade, and social media assess availability. This information could assist in further drawing conclusions as to the level of training needed for individual Marines.

Appendix (A):

MSS Questionnaire:
This questionnaire supports a thesis for a master's degree in Military Studies at the Command and Staff College, Marine Corps University. The focus of the thesis is how the Marine Corps' acceptance of social media has affected the Corps operations security. Your honest responses to the below questions will be kept in complete anonymity and will be used for the purpose of this educational research. The expected time to complete the questionnaire is about 15 minutes.

1) Have you taken a PII instructional course via the computer?

- ☐ No (skip to question 3)
- ☐ Yes

2) Did you learn anything you didn't already know from the course?

- ☐ No
- ☐ Yes

3) Do you feel you require further PII and OPSEC training?

- ☐ No
- ☐ Yes

4) Do you use social networking sites (SNS)?

- ☐ No
- ☐ Yes - I only use 1 site
- ☐ Yes – I use between 2 and 5 sites
- ☐ Yes – I use more than 5 sides

5) How often do you access these sites?

- ☐ none at all
- ☐ 1 time a day
- ☐ More than 1 time a day
- ☐ about once a week

6) Do you utilize SNS on official computers (on and off duty)?

- ☐ No
- ☐ Yes

7) Do you utilize operations security (OPSEC) while viewing and interacting on SNS?

- ☐ No
- ☐ Yes

8) Do you currently post to blogs?

- ☐ No
- ☐ Yes - I only use 1
- ☐ Yes – I use between 2 and 5
- ☐ Yes – I use more then 5

9) When you post online do you:
    - Use your real name? (Yes)
    - Use identifying usernames i.e. MAGTF1? (Yes)
    - Post your military/government affiliations? (Yes)
    - Provide Personal Information:
        i. Hometown (Yes)
        ii. Schools (Yes)
        iii. Deployments (Yes)
        iv. Personal associations (Yes)
        v. Names of friends (Yes)
        vi. Duty Stations (Yes)
        vii. Military Units (Yes)
        viii. Training (Yes)

10) What is your understanding of OPSEC and SNS?

11) How can the Marine Corps increase awareness of OPSEC?

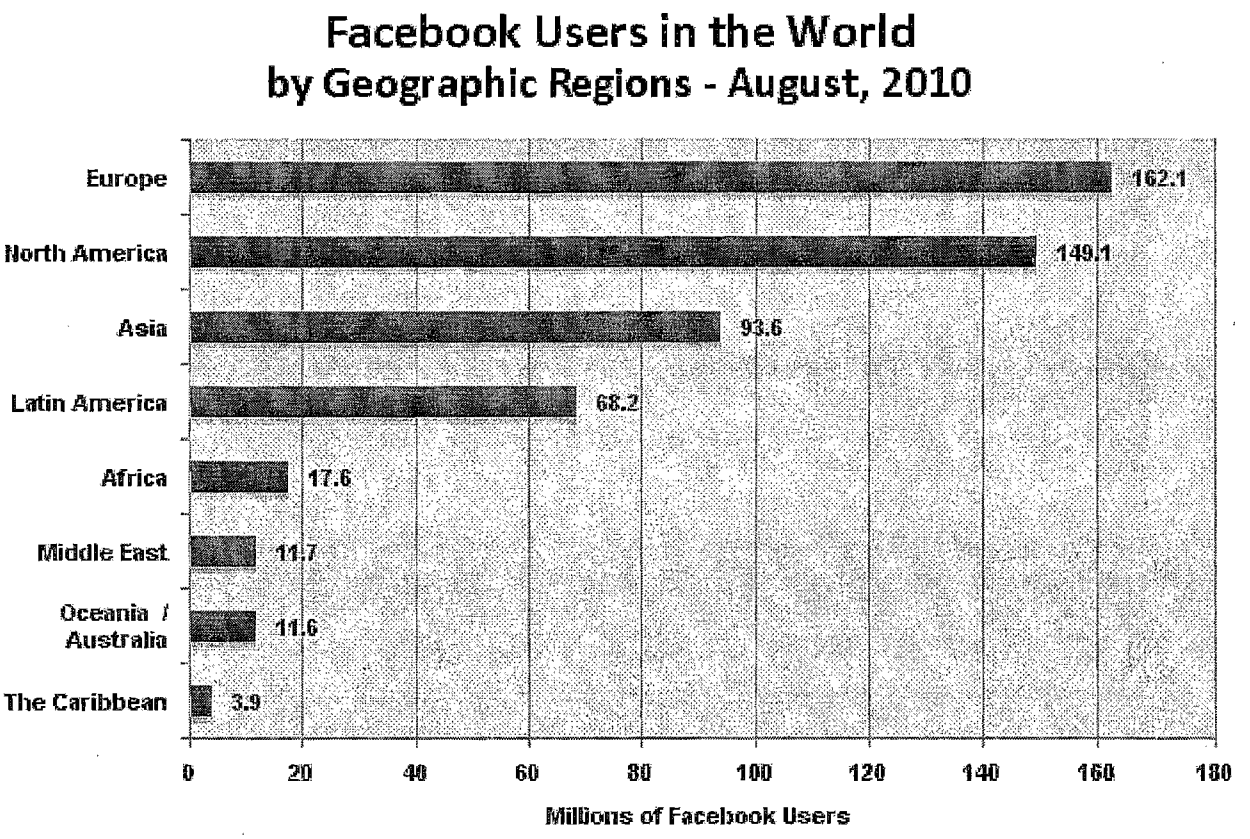
Appendix (B):

INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	**110,931,700**	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	**825,094,396**	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	**475,069,448**	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	**63,240,946**	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	**266,224,500**	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	**204,689,836**	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	**21,263,990**	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	**1,966,514,816**	**28.7 %**	444.8 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2010. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com.

Appendix (C):



Source: Internet World Stats - www.internetworldstats.com/stats25.htm
Estimated Facebook users were 517,760,460 on August 31, 2010
Copyright © 2010, Miniwatts Marketing Group

Bibliography:

(2008, 01 06). Retrieved 12 12, 2010, from Merriam-Webster Online Dictionary: http://www.merriam-webster.com

Alexa Internet, I. (2010). *Top Sites in United States* . Alexa Internet, Inc.

Department of Defense. (2011, February 3). *Social Media Sites*. Retrieved January 2, 2011, from US Department of Defense: http://www.defense.gov/registeredsites/socialmediasites.aspx

FaceBook Users in the World. (2010, August 31). Retrieved January 13, 2011, from Internet World Stats: http://www.internetworldstats.com/stats25.htm

Graham, I. (2009, August 6). *DoD Live: DoD and Marine Corps Speak Out on Social Media Ban*. Retrieved Novemeber 13, 2010, from DoD Live: http://www.dodlive.mil/index.php/2009/08/dod-and-marine-corps-speak-out-on-social-media/#

Kane, S. (2010). *Gereration Y*. Retrieved January 19, 2011, from About/com: http://legalcareers.about.com/od/practicetips/a/GenerationY.htm

Lipowicz, A. (2010, November 17). VA reports on social media, software development. Washington, DC, United States of America.

Lynn, William. *Responsible and Effective Use of Internet-Based Capabilities*. Memorandom, Washington, DC: Department of Defense, 2010.

Navy wants to grow sailors' brains with iPhone app. (2010, November 12). Retrieved December 02, 2010, from Federal News Radio: http://www.federalnewsradio.com/?nid=150&sid=2116320

Schmidt, C. S. (2010, 04 08). *Marines.mil*. Retrieved 11 20, 2010, from Social media: changing how the Marine Corps operates : http://www.marines.mil/unit/hqmc/Pages/SocialmediachanginghowtheMarineCorpsoperates.aspx

Service, A. S. (2009). U.S. Forces Afghanistan Surpasses 20,000 Facebook Fans. *Defense.gov* , 1-3.

Tucker, Jennifer. "Mobile Learning Approaches for U.S. Army Training." Research Note, Fort Benning, 2010.

Tyson, M. (2010, March 8). Wii-hab: Veterns get more then fun with Wii-hab. Washington, DC, United States of America.

World Internet Users and Population. (2010, August 1). Retrieved January 12, 2011, from Internet World Stats: http://www.internetworldstats.com/stats.htm

Magazines:

King, R. (2009, August 4). *U.S. Marine Corps bans Social Networking Sites.* Retrieved November 22, 2010, from Bloomburg Businessweek: http://www.businessweek.com/technology/technology_at_work/archives/2009/08/us_marine_corps_bans_social_networking_sites.html

Tom Budzyna, D. o. (2010, August 31). Social Media Shapes Markets, the Military and Life. *American Forces Press Service* , pp. 1-3.

United States Marine Corps Regulations:

Commadant of the Marine Corps. (2007, May 18). THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM. *MCO 3070.2* .

Williams, W. J. (2010, March 29). Responsible and effective use of internet-based capabilities . Quantico, Virginia, United States of America.

Marines.MIL. (2011, February 3). *Marine Corps Social Media.* Retrieved January 21, 2011, from Marines.mil: http://www.marines.mil/usmc/Pages/SocialMedia.aspx

Allen, G. J. (2009, August 03). Immediate ban of internet social networking sites (SNS) on Marines Coprs Enterprise network (MCEN) NIPRNET. Quantico, Virginia, United States of America.

Flynn, G. J. (2010, September 23). TESTIMONY TO THE TERRORISM, UNCONVENTIONAL THREATS, AND CAPABLITIES SUBCOMMITTEE ON THREATS, AND CAPBILITIES SUBCOMMITTE ON OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY DEPARTMENTS FOR CYBER OPERATIONS. 2-6. Washington, DC, United States of America.

---

[1] (Internet World Stats: Facebook Statistics 2010)
[2] (Alexa Internet 2010)
[3] (Allen 2009)
[4] (Lipowicz 2010)
[5] (Merriam-Webster Online Dictionary 2008)
[6] (OsiXs 2006)
[7] (Merriam-Webster Online Dictionary 2008)
[8] (Flynn 2010)
[9] (National Journal Staff 2011)

[10] (O'Reilly 2005)
[11] (Wong 2011)
[12] (Tom Budzyna 2010)
[13] (Allen 2009)
[14] (Williams 2010)
[15] (Sharp 2009)
[16] (Kane 2010)
[17] (Marines 2010)
[18] (Associated Press 2010)
[19] (World Internet Users and Population 2010)
[20] (FaceBook Users in the World 2010)
[21] (Military.com 2008)
[22] (Navy wants to grow sailors' brains with iPhone app 2010)
[23] (Pellerin 2010)
[24] (Sharp 2009)
[25] (Allen 2009)
[26] (King 2009)
[27] (King 2009)
[28] (Graham 2009)
[29] (Graham 2009)
[30] (Graham 2009)
[31] (Schmidt 2010)
[32] (Williams 2010)
[33] (Tom Budzyna 2010)
[34] (Department of Defense 2011)
[35] (U.S. Forces Afghanistan Surpasses 20,000 Facebook Fans 2009)
[36] (U.S. Forces Afghanistan Surpasses 20,000 Facebook Fans 2009)
[37] (Janes 2009)